pending claims under the above combination of Hasebe #1, Hasebe #2, and Iwayama et al. references.

The Present Invention

The present claimed invention is directed to a system for protecting data against unauthorized use. While data may be initially authorized for use by a particular user, the subsequent use of that data is not necessarily also authorized for use. The present invention prevents such unauthorized use by determining whether the data being processed is data that requires prior authorization for use and determining the nature of the processing to be performed on the data. For example, storage of the original data requiring authorization is forbidden by the system to prevent subsequent unauthorized use of the data. Cut and paste operations on the protected data are also blocked by the present invention. Processed data that includes data requiring authorization for use can be subsequently distributed as data requiring authorization for use, thereby continuing the protection of the original data.

The Hasebe #1 Reference

Hasebe #1 discloses a data protection system for preventing unauthorized copying of electronic data, such as computer software (Hasebe #1 at abstract, Col. 1, lines 6 - 9). The protected software is provided to the user encrypted on a storage medium such as an optical disk (Col. 1, lines 63 - 65; Col. 2, lines 27 - 29). The electronic key for decrypting the data is stored on the storage medium in encrypted form (Col. 1, line 66 - Col. 2, line 3). The vendor computer supplies encrypted permission information, for decrypting the encrypted electronic data, to the user computer via transmission or to the user in a document (Col. 2, lines 14 - 26). Upon decryption, the unencrypted software is available for execution by the user (Col. 3, lines 37 - 39; Col. 5, line 66 - Col. 6, line 2).

The Hasebe #2 Reference

Hasebe #2 discloses a system for charging for use of digitized data such as software and for granting permission to use the data (Hasebe #2 at abstract; Col. 1, lines 7 - 9). The supplied data is decrypted for use by a software managing module (Col. 3, lines 46 - 65). Deciphering for subsequent use by the user is permitted only if an available credit balance exists in a charging table (Col. 4, lines 18 - 21). The available balance is subtracted based on the deciphering processing amount or the processing period of time for the ciphered software data (Col. 4, lines 23 - 25). The user can add to the remaining balance total to permit additional use of the data (Col. 4, lines 25 - 29).

The Iwayama et al. Reference

Iwayama et al. discloses a system for authorized accessing of encoded electronic data such as computer software (Iwayama et al. at abstract; Col. 2, lines 11 - 15). The data is first stored as encoded data on a storage medium such as a compact disk (Col. 2, lines 30 - 33). The desired portion of encoded data will be decoded when a user inputs the identification information for the preferred data content (Col. 2, lines 61 - 65). When the decoding is completed, the system compares the decoded content identification information with the user-supplied content information (Col. 3, lines 14 - 19). If the two sets of information match, the system will output the selected data portion to the user (Col. 3, lines 19 - 22).

The Present Invention Patentably Distinguishes Over the Prior Art

The present claimed invention, as recited in claim 1, is directed toward a data protection system for protecting input data that requires authorization for use. The system generates information relating to the input data, appends the generated information to prepared data, and displays the resultant appended data. Each of the three references cited by the Examiner merely allow the unmodified use of the protected, encrypted electronic data once the permission or authorization key has been provided to or by the user. In particular, Hasebe #1 permits simple execution of the protected software (Hasebe #1 at Col. 3, lines 37 - 39); Hasebe #2 allows use of

the software if sufficient balance remains in the charge account (Hasebe #2 at Col. 4, lines 25 - 29); and Iwayana et al. outputs the music or software to the user for playing or execution upon matching the decoded content and user content identification information (Iwayama et al. at Col. 2, lines 21 - 23; Col. 3, lines 14 - 22). None of these references disclose or suggest the claimed feature of appending protected data to user-prepared data and subsequently displaying the appended data. The portion of Hasebe #1 relied upon by the Examiner to allegedly teach preparing data merely discloses making the "plain text software" available for "load[ing] into a main storage of the user computer," which is not the preparation disclosed and claimed herein. As regards the claimed feature of appending the generated information to the prepared data, claim 12 of Hasebe #2, as relied upon by the Examiner, discloses an authorization center adding a utilization key to the software data, not the appending of generated information to prepared data. As regards displaying the appended data, Fig. 4 of Iwayama et al. and Fig. 2 of Hasebe #2, as relied upon by the Examiner, disclose only means to display the unmodified protected data. The present invention further includes the feature of preventing the storage of the input data, wherein said input data is judged to be data requiring authorization for use. The Examiner admits that the prior art does not teach such a feature, but has asserted that forbidding saving is well known in the art as a decision-making/query instruction. The Applicants respectfully traverse the Examiner's assertion that it would have been obvious to include such a feature and request the Examiner cite a reference supporting the assertion in the present art of systems for protecting data from unauthorized use, pursuant to MPEP §2144.03.

While teachings of several references may be combined by the Examiner to render a claimed invention obvious, there must be a motivation or suggestion in the prior art to make the specific combination (In re Oetiker, 24 USPQ2d 1443, 1447 (CAFC 1992); In re Fritch, 23 USPQ2d 1780, 1783 (CAFC 1992)). The Applicants respectfully assert that no suggestion or motivation exists in Hasebe #1, Hasebe #2, or Iwayama et al. to combine the specific features of data protection disclosed in each reference to create the present claimed invention. In particular, each reference teaches a separate, specific means of granting permission for use of the electronic

data. The Applicants respectively assert that picking and choosing among the features relied upon by the various references would actually defeat the protection system taught by the respective patents; and that by so doing, the Examiner has improperly relied upon the disclosure herein as a template to piece together prior teachings in an attempt to render the invention obvious. *In re Fritch*, 23 USPQ2d 1780, 1783-84 (CAFC 1992).

Claim 2 depends from claim 1 and includes all the limitations of claim 1 plus additional limitations which are not taught or suggested by the prior art. In particular, claim 2 recites means for executing a cut and paste function with respect to the input data, and means for preventing the cut and paste function with respect to the input data when the input data is data requiring authorization for use. As admitted by the Examiner, none of the references disclose such features. Therefore, for at least this reason and the reasons set forth above with respect to claim 1, it is submitted that claim 2 patentably distinguishes over the prior art. The Applicants respectfully traverse the Examiner's assertion that it would have been obvious to include such manipulation and forbidding means in the present invention. While cut and paste features may be known in the general art of data processing, the Applicants respectfully submit that their invention is novel regarding preventing a cut and paste operation on data requiring authorization for use. Therefore, the Applicants respectfully request the Examiner cite a reference supporting the assertion in the present art of systems for protecting data from unauthorized use, pursuant to MPEP §2144.03.

Claim 3 depends from claim 1 and includes all the limitations of that claim plus additional limitations. Therefore, for at least the reasons cited above with respect to claim 1, it is submitted that claim 3 patentably distinguishes over the prior art.

Independent claims 4 and 9 recite the additional feature of storage means storing process information indicating what kind of processing has been applied to the data by the processing means. Each of the references disclose mere use of the decrypted electronic data rather than subsequent processing of the electronic data; and, therefore, none of the references disclose any information regarding what processing is applied to the data, much less the storing of such

information.

Claims 5 - 8 and 10 - 11 depend from claims 4 and 9, respectively, and include all the limitations of those claims plus additional limitations. Therefore, for at least the reasons cited above with respect to claims 4 and 9, it is submitted that claims 5 - 8 and 10 - 11 patentably distinguish over the prior art.

Independent claims 12 and 15 recite the additional feature of permitting the use of data for a charge wherein the data requires authorization for use. While the Examiner has failed to address this limitation, contrary to the requirements of MPEP §706.02(j), the Applicants note that only Hasebe #2 provides for charging for the software data. However, as discussed above regarding claim 1, and as recited by claim 12, Hasebe #2 fails to disclose appending means appending the generated information to the prepared data, and display means displaying the prepared data and the input data in the appended condition. Furthermore, as discussed above regarding claims 4 and 9, and as recited by claim 15, Hasebe #2 fails to disclose storage means storing process information indicating what kind of processing has been applied by the processing means.

Claims 13 - 14 and 16 - 17 depend from claims 12 and 15, respectively, and include all the limitations of those claims plus additional limitations. Therefore, for at least the reasons cited above with respect to claims 12 and 15, it is submitted that claims 13 - 14 and 16 - 17 patentably distinguish over the prior art.

New Claims

Claims 18 - 21 have been added to provide additional claim coverage for the present invention). The prior art of record does not teach or suggest a system for protecting data against unauthorized use which includes inputting the protected data, processing the data to produce generated data, and preventing the storage of the generated data as set forth in claims 18 and 19. The prior art of record also does not teach or suggest a system for protecting data against unauthorized use which includes inputting or storing the protected data, processing the data, and

storing the process information indicating what kind of processing has been applied by the processing means as set forth in claims 20 and 21.

Summary

It is submitted that none of the references, either taken alone or in combination, teach the present claimed invention. Thus, claims 1 - 21 are deemed to be in a condition suitable for allowance. Reconsideration of the claims and an early Notice of Allowance are earnestly solicited. If any fees are required in connection with the filing of this Amendment, please charge same to Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY, LLP

By: David M. Pitcher Reg. 25,908
John C. Garvey
Reg. No. 28,607

700 Eleventh St., N.W., Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501
Date: December 29, 1999

(W:\1083\1048\AMEND1)

CERTIFICATE UNDER 37 CFR 1.8(a)

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D.C. 20231

on December 29, 1999

STAAS & HALSEY

By: Valerie A. Purdy

Date: December 29, 1999